MARKED-UP VERSION

53. (Once Amended) A computer readable medium containing program instructions for a software toolkit containing a collection of data structures and subroutines for developing an application for playing digital content data, the program instructions comprising instructions for:

receiving previously encrypted content data encrypted with an encryption key from an external source;

decrypting the received previously encrypted content data;

reencrypting the decrypted received content data with a local encrypting key wherein the local encrypting key is a type of encryption key which enables streaming playback of the encrypted content while the encrypted content is being decrypted and without the need to first decrypt the entire encrypted content;

storing the previously encrypted content data in a library;

selecting one or more encrypted content data from the library to play; and

decrypting each content data selected to be played with its unique decryption key,

wherein the decrypting is performed in a tamper-resistant subroutine for deterring unauthorized access to the instructions for decrypting the content data and for deterring unauthorized access to the decryption key; and;

wherein the decrypting and reencrypting instructions are performed in the tamper resistance subroutine.

54. (Once Amended) The computer readable medium according to claim 53, wherein the step of [further including instructions for:

decrypting the received previously encrypted content data prior to storage in the library;]

reencrypting the decrypted received content data with a local encrypting key includes encrypting with IBM's SEAL algorithm

[wherein the decrypting and reencrypting instructions are performed in the tamper resistance subroutine].

55. (Once amended) The computer readable medium according to claim 5[4]3, wherein the instruction for reencrypting the decrypted received content data utilizes a unique local decrypting key for each content data prior to storage in the library.

73. (Once Amended) A method for providing a collection of data structures and subroutines for developing an application for playing digital content data, the method comprising the steps of:

receiving previously encrypted content data encrypted with an encrypted key from an external source;

decrypting the received previously encrypted content data;

reencrypting the decrypted received content data with a local encrypting key wherein the local encrypting key is a type of encryption key which enables streaming playback of the encrypted content while the encrypted content is being decrypted and without the need to first decrypt the entire encrypted content;

storing the previously encrypted content data in a library;

selecting one or more encrypted content data from the library to play; and

decrypting each content data selected to be played with its unique decrypting key;

wherein the decrypting is performed in a tamper-resistant subroutine for deterring unauthorized access to the instructions for decrypting the content data and for deterring unauthorized access to the decrypting key; and

wherein the decrypting and reencrypting instructions are performed in the tamper resistance subroutine.

74. (Once Amended) The method according to claim 73, further comprising the step of:

decrypting the received previously encrypted content data prior to storage in the library;

reencrypting the decrypted received content data with a local encrypting key includes encrypting with IBM's SEAL algorithm

[wherein the decrypting and reencrypting instructions are performed in the tamper resistance subroutine].

75. (Once Amended) The method according to claim 7[3]4, wherein the step for reencrypting the decrypted received content data utilizes a unique local decrypting key for each content data prior to storage in the library.

83. (New) An end user device for rendering encrypted content comprising:

an interface to a computer readable medium for receiving previously encrypted content data encrypted with an encrypted with a key from an external source;

an interface to a library for storage of the content;

a software application for

decrypting the received previously encrypted content;

reencrypting the decrypted received content data with a local encrypting key wherein the local encrypting key is a type of encryption key which enables streaming playback of the encrypted content while the encrypted content is being decrypted and without the need to first decrypt the entire encrypted content; and

storing the previously encrypted content data in the library;

a user interface for selecting one or more encrypted content data from the library to play; and

a tamper resistant environment which deterring unauthorized access to the instructions for decrypting the content data and for deterring unauthorized access to the decrypting key, whereby inside the tamper resistant environment each content data selected to be played is decrypted with its unique decrypting key; and

wherein the decrypting and reencrypting instructions are performed in the tamper resistance environment.

84. (New) The end user device according to claim 83, wherein the local encrypting key includes IBM's SEAL algorithm.

85. (New) The end user device according to claim 83, wherein the local encrypting key includes a unique local encryption key for each content data prior to storage in the library.

86. (New) The end user device according to claim 85, wherein the software application stores the unique local encryption key in several distinct parts throughout an information processing system.

87. (New) The end user device according to claim 84, wherein the software application stores the common local encryption key in several distinct parts throughout an information processing system.

REMARKS

Applicants have studied the Office Action dated Office Action dated June 27, 2001 (paper no. 12) and have made amendments to the claims. It is submitted that the application, as amended, is in condition for allowance. By virtue of this amendment, claims 53 - 62 and 73 - 87 are pending. Claims 83 - 87 have been added. Reconsideration and allowance of the pending claims in view of the above amendments and the following remarks are respectfully requested. In the Office Action, the Examiner:

- rejected claims 53 - 62 and 73 - 82 under 35 U.S.C. § 102(e) as being anticipated by Ginter et al, (U.S. 5,892,170).

Overview of the Current Invention

Preferred Embodiments of the present invention provide an improved method, apparatus and computer readable medium to manage electronic digital content on end-user devices. The present invention provides a set of tools that can handle the decryption of the digital content in a tamper resistant environment, that is, an environment to deter the unauthorized access to the content being played on an end user device. In addition, the present invention provides a local reencryption process that permits faster access to encrypted data and that permits the encrypted content to be deencrypted in a stream while playing. This is unlike the prior art systems that require the entire content to be decrypted prior to being played. This minimizes the exposure of decrypted content while the content is played because only a very small portion of the encrypted content is decrypted during playback. As stated in the specification o the present invention in the section entitled "C. Secure Container Processor 192" page 133 and more generally pages 131 - 135 (Emphasis added)

> "The process of Decryption and Re-Encryption 194 serves two purposes. Storing the Content 113 encrypted with an algorithm like SEAL enables faster than real-time decryption and requires much less processor utilization to perform the decryption than does a more industry standard type algorithm like DES. This enables the Player Application 195 to perform a real-time concurrent decryption-decode-playback of the Content 113 while the encrypted content is being

decrypted and without the need to first decrypt the entire file for the Content 113 prior to decode and playback. The efficiency of the SEAL algorithm and a highly efficient decode algorithm, allows not only concurrent operation (streaming playback from the encrypted file) but also allows this process to occur on a much lower powered system processor. Thus this application can be supported on a End-User Device(s) 109 as low end as a 60MHz Pentium system and perhaps lower. Separating the encryption format in which the Content 113 is finally stored from the original encryption format, allows for greater flexibility in the selection of the original content encryption algorithm. Thus use of widely accepted and proven industry standard algorithms can be used thus further enhancing Digital Content Industry acceptance of the Secure Digital Content Electronic Distribution System 100.

Unlike prior art systems the local reencrypting and encryption process uses a type of encryption key which enables streaming playback of the encrypted content while the encrypted content is being decrypted and without the need to first decrypt the entire encrypted content.

In order to more particularly point out these features of: a type of encryption key which enables streaming playback of the encrypted content while the encrypted content is being decrypted and without the need to first decrypt the entire encrypted content, the following language has been added the independent claims, i.e., claims 53, 73, and 83 as follows [1]:

- Claims 53 and 73

  reencrypting the decrypted received content data with a local encrypting key wherein the local encrypting key is a type of encryption key which enables streaming playback of the encrypted content while the encrypted content is being decrypted and without the need to first decrypt the entire encrypted content;

- Claim 83

  a software application for

[1] See §2173.05(i) Negative limitations in claims is not wrong so long as the boundaries of the patent protection sought are set forth definitely as they are here in the present invention.

decrypting the received previously encrypted content; and for

reencrypting the decrypted received content data with a local encrypting key wherein the local encrypting key is a type of encryption key which enables streaming playback of the encrypted content while the encrypted content is being decrypted and without the need to first decrypt the entire encrypted content;

Rejection under 35 U.S.C. §102(e)

As noted above, rejected claims 53 - 62 and 73 - 82 under 35 U.S.C. § 102(e) as being anticipated by Ginter et al, (U.S. 5,892,170). Independent claims 53, 73, and 83 have been amended to distinguish over Ginter. The Examiner at pages 2 and 3 of the office action states *"Regarding claim 73, Ginter discloses [...] decrypting each content data selected to be played with its unique decrypting key, wherein the decrypting is performed in a tamper-resistant subroutine for deterring unauthorized access to the instructions for decrypting the content data and for deterring unauthorized access to the decrypting key (column 195, lines 27-47 and column 64, line 15-40) [...] Regarding claim 74, Ginter further discloses decrypting the received previously encrypted content data prior to storage in the library; re-encrypting the decrypted receive content data with a local encryption key wherein the decrypting and re-encrypting instructions are preformed in the tamper resistant subroutine (columns 170-172)."* However, careful reading of Ginter discloses reencrypting the entire item in the database. Or in the words of Ginter: "The keys to decrypt secure database 610 records are, in the preferred embodiment, maintained solely within the protected memory of an SPU 500. Each index or record update that leaves the SPU 500 may be time stamped, and then encrypted with a unique key that is determined by the SPE 503." See Ginter at Col. 171 lines 14-16 and FIG. 37. This is not the same as using reencrypting the decrypted received content data with a local encrypting key wherein the local encrypting key is a type of encryption key which enables streaming playback of the encrypted content while the encrypted content is being decrypted and without the need to first decrypt the entire encrypted content.[2] In fact, Ginter teaches exactly the problem in the

[2] See §2173.05(i) Negative limitations in claims is not wrong so long as the boundaries of the patent protection sought are set forth definitely as they are here in the present invention.

prior art of decrypting and reencrypting using DES type keys and the use of proprietary hardware for a tamper resistant environment. See Ginter FIG. 6 and Col. 22, Lines 1 -14. The present invention provides reencrypting with an efficient algorithm, such as IBM's SEAL algorithm, and a highly efficient decode algorithm. Using this type of encryption and corresponding decryption, permits the present invention to concurrently operate (streaming playback from the encrypted file) and moreover provides a decryption system which is able to operate on a lower-powered system (i.e., lower processor power) without the use of specialized hardware such as the secure processing environment (SPE) 503 of Ginter. This is important because the present invention enables an encrypted playback solution to scale from low-power end-user systems, such as Palm Pilot, up through higher power desktop systems. See Present Invention as entitled "C. Secure Container Processor 192" pages 133 (Emphasis added). Moreover, the present invention further provides greater flexibility by allowing for one type of encryption, such as DES, to be used when transmitting and receiving the encrypted content to the end-user device and another type of encryption to be used on low-powered devices to enable concurrent decryption and playback. Accordingly, the present invention independent claims 53, 73, and 84 distinguishes over Ginter for at least this reason.

Independent claims 53, 73, and 83 have been amended to distinguish over Ginter. Claims 54 - 62, 74 - 83, and 85 87, depend from claims 53, 73, and 83 respectively and since dependent claims contain all the limitations of the independent claims, claims 53-62, and 74 - 87 distinguish over Ginter, as well.

The Examiner cites 35 U.S.C. § 102(b) and a proper rejection requires that a single reference teach (i.e., identically describe) each and every element of the rejected claims as being anticipated by Ginter.[3] The elements in independent claims 53, 73, and 84 of "reencrypting the decrypted received content data with a local encrypting key wherein the local encrypting key is a type of

[3] See MPEP §2131 (Emphasis Added) "A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). "The identical invention must be shown in as complete detail as is contained in the ... claim."

encryption key which enables streaming playback of the encrypted content while the encrypted content is being decrypted and without the need to first decrypt the entire encrypted content" is not taught or disclosed by Ginter. The apparatus of Ginter does not allow streaming playback of the encrypted content because the entire encrypted content must be decrypted in Ginter. The Applicants respectfully submitted that the Examiner's rejection under 35 U.S.C. § 102(b) have been overcome.

Moreover, dependent claims 54, 74, and 84 "wherein the local encrypting key includes IBM's SEAL algorithm." This technology is no where taught or suggested by Ginter and instead Ginter teaches DES type encryption algorithms which do not provide the same results of the IBM SEAL algorithm of low processor requirement and concurrent decryption of a content stream when the stream is being played. This is not possible with DES type algorithms since the entire encrypted content must be decrypted all at once. Accordingly, independent claims 54, 74, and 84 distinguish over Ginter for at least this reason as well.

CONCLUSION

Independent claims 53 ans 73 have been amended. Independent claim 84 added. All the remaining claims dependent from the amended claims. In view of the foregoing, Applicants respectfully submits that all of the grounds for rejection stated in the Examiner's office action have been overcome, and that all claims in the application are allowable. No new matter has been added. It is believed that the application is now in condition for allowance, which allowance is respectfully requested.

PLEASE CALL the undersigned if that would expedite the prosecution of this application.

Respectfully submitted.

By: _____

Jon Gibbons (Reg. No. 37,333)
Attorney for Applicant
Fleit, Kain, Gibbons, Gutman & Bongini, P.L.
One Boca Commerce Center, Suite 111
551 N.W. 77th Street
Boca Raton, FL 33487
Tel. (561) 989-9811
Fax (561) 989-9812

PLEASE Direct All Correspondence to Customer Number 23334

150-a99-062amend1.wpd